

Arcserve Cloud Direct スタートアップ ガイド

【Windows 編】

本資料は、Arcserve Cloud Direct の製品概要をご理解した方向けに、物理の Windows 環境を保護するための設定手順を記載したガイドです。

他の構成のためには以下のガイドもご用意しています。

- ◆ Arcserve Cloud Direct スタートアップ ガイド 【仮想エージェントレス編】

<https://www.arcserve.com/sites/default/files/wp-doc/ucd-startup-guide-agentless.pdf>

- ◆ Arcserve Cloud Direct スタートアップ ガイド 【Linux 編】

<https://www.arcserve.com/sites/default/files/wp-doc/ucd-startup-guide-linux.pdf>

Arcserve Cloud Direct の製品概要については、下記をご参照ください。

- ◆ Arcserve Cloud Direct 紹介資料

<https://www.arcserve.com/sites/default/files/wp-doc/ucd-presentation.pdf>

Arcserve Cloud Direct はクラウド サービスであり、管理 UI は自動的に更新されます。

そのため、本ガイドに掲載されている画面ショットや一部の操作は実環境と異なる場合がございます。

本資料中に記載のある「DRaaS」は新規の販売を終了しております。



改訂履歴

- 2019年8月 Rev1.0 リリース
- 2019年9月 Rev1.1 リリース
- 表紙に他のガイドの案内追記
 - 画面ショット更新
- 2019年11月 Rev1.2 リリース
- クラウド側のストレージ消費量についての表記修正
- 2020年3月 Rev1.3 リリース
- フェイルバックに関する追記
 - トライアル開始方法の変更に伴う修正
- 2020年4月 Rev1.4 リリース
- ライセンス購入時にも[トライアル開始]をクリックする旨を追記
- 2020年7月 Rev1.5 リリース
- 東日本リージョン開設に伴う修正
 - タスクの設定に機能追加
 - 一部 URL のリンク切れ修正
- 2020年10月 Rev1.6 リリース
- SPEED TEST サイトに東日本リージョンが追加されたことに伴う修正
 - Arcserve UDP 変更トラッキングドライバとの競合についての情報追加
 - エージェントの Web プロキシ設定追加
 - UI に Exchange が追加されたことに伴う修正
- 2021年3月 Rev1.7 リリース
- UI の全体的な変更にもとない手順の文言変更、スクリーンショット貼り替え
 - トライアルについて注意書きを追記
- 2021年7月 Rev1.8 リリース
- 利用する通信ポートの追記、表現修正
 - BaaS の保存期間に 2 か月、3 か月、6 か月を追加
 - BaaS のディスク全体バックアップの増分で時間がかかる場合があることを記載
 - DRaaS のプロビジョニングによりバックアップ運用が停止する旨を追記
 - [トライアル版の開始]についての注意の文言微修正
- 2021年11月 Rev1.9 リリース
- 2 要素認証に関する記述追加
 - プロキシのアカウント設定について補足
 - リストアの補足として、システムブートは不可な旨を追記
 - アイコン変更
 - UNC パス指定によるバックアップが可能なことを追記

- 2022年1月 Rev1.91 リリース
- ライセンス登録の時差計算の誤りを修正
- 2022年6月 Rev1.92 リリース
- 「フル システム」「ドライブの選択」画面表記変更に伴う修正
- 2023年1月 Rev2.0 リリース
- 新 Cloud Console への移行による UI 変更に伴う修正
 - 製品名を変更
 - 旧名称: Arcserve UDP Cloud Direct
 - 新名称: Arcserve Cloud Direct
- 2023年2月 Rev2.1 リリース
- 仮想エージェントレス編、Linux 編と表記を合わせるための軽微な文言修正、
 - 一部スクショ更新
 - 価格表やガイドなどの URL 修正
- 2023年2月 Rev2.2 リリース
- Arcserve アカウント登録手順修正（フルフィルメント ID、注文番号入力 不要）
- 2023年3月 Rev2.3 リリース
- AD Option 関連記述削除
- 2023年7月 Rev2.4 リリース
- ライセンス プログラム証書の送信元、件名修正
 - Cloud Console のアクセス許可設定について追記
- 2023年9月 Rev2.5 リリース
- ネットワーク要件修正
- 2023年10月 Rev2.6 リリース
- DRaaS 終売の旨を記載
- 2023年12月 Rev2.7 リリース
- 通信に使用するポートについての記述修正

目次

Arcserve Cloud Direct スタートアップ ガイド	1
目次	4
1 用語と構成例	6
1.1 用語の説明.....	6
1.2 使用するコンポーネント.....	6
1.3 Windows 環境のバックアップ構成例.....	8
2 事前確認	9
2.1 Arcserve Cloud Direct 環境構築の流れ.....	9
2.2 動作要件、その他要件の確認.....	9
3 Arcserve アカウントの登録とライセンス有効化.....	11
3.1 Arcserve アカウントの登録.....	11
3.2 Cloud Console へのアクセスとライセンスの有効化	21
3.3 DRaaS 設定のサポート依頼.....	27
4 コンポーネントの導入.....	28
4.1 必要なコンポーネントのダウンロード	28
4.2 Windows 用 Agent のインストール.....	29
5 バックアップの設定	35
5.1 バックアップ先ボリュームの作成	35
5.2 ポリシー作成の開始	37
5.3 基本情報の設定	37
5.4 ソースの設定	38
5.5 タスクの設定.....	39
5.5.1. 保護対象の設定.....	39
<参考：アクティビティのタイプとリストア単位>	42

5.5.2.	保護する場所の設定	43
5.5.3.	保護するタイミングの設定	44
5.5.4.	追加の設定	45
5.6	ポリシー設定の完了	45
5.7	バックアップ結果の確認	46
5.8	タスクの追加、変更、削除	47
5.8.1.	タスクの追加方法	47
5.8.2.	タスクの削除方法	48
6	データのリストア	49
6.1	フォルダのリストア	49
6.2	イメージのリストア	53
7	Arcserve クラウドに復旧された VM へのアクセス	54
7.1	プロビジョニングの実施	54
7.2	復旧された VM へのリモート デスクトップ接続	55
7.3	ポイント対サイト (Point to Site) の VPN 接続	58
8	通常運用環境への切り戻し	60
8.1	フェイルバックの実行	60
9	参考情報	63

すべての製品名、サービス名、会社名およびロゴは、各社の商標、または登録商標です。

本ガイドは情報提供のみを目的としています。Arcserve は本情報の正確性または完全性に対して一切の責任を負いません。Arcserve は、該当する法律が許す範囲で、いかなる種類の保証（商品性、特定の目的に対する適合性または非侵害に関する黙示の保証を含みます（ただし、これに限定されません））も伴わずに、このドキュメントを「現状有姿で」提供します。Arcserve は、利益損失、投資損失、事業中断、営業権の喪失、またはデータの喪失など（ただし、これに限定されません）、このドキュメントに関連する直接損害または間接損害については、Arcserve がその損害の可能性の通知を明示的に受けていた場合であっても一切の責任を負いません。

© 2023 Arcserve (USA), LLC. All rights reserved.

1 用語と構成例

1.1 用語の説明

- Arcserve Business Continuity Cloud

Arcserve が提供するデータ保護サービスの総称です。Arcserve Cloud Direct と Arcserve UDP Cloud Hybrid の 2 種類のサービスで構成されています。「Arcserve クラウド」と省略されることもあります。

- Arcserve Cloud Direct

本書で説明するバックアップ サービスです。「Cloud Direct」と省略されることもあります。

- BaaS (Backup as a Service : バックアップ サービス)

Arcserve Cloud Direct のバックアップ/リストア機能だけを使う方式です。

- DRaaS (Disaster Recovery as a Service : 惨事復旧サービス)

バックアップ/リストアに加えて、本番システムの代替仮想マシンを Arcserve クラウド上で起動できる方式です。

1.2 使用するコンポーネント

◆BaaS/DRaaS 共通

- Arcserve Cloud Console (以下 Cloud Console)

Web ブラウザで利用するクラウド ベースの管理 UI です。

Arcserve Cloud の HOME 画面からアクセスします。

Arcserve Cloud Direct のコンポーネントのダウンロード、バックアップ設定、リストア、ジョブ監視等の管理に利用します。

- Arcserve Cloud Direct Agent (以下 Cloud Direct エージェント)

バックアップ対象に導入するプログラムで、バックアップ データを Arcserve クラウドに転送します。Windows 用と Linux 用があります。Replication Agent と呼ぶ事もあります。

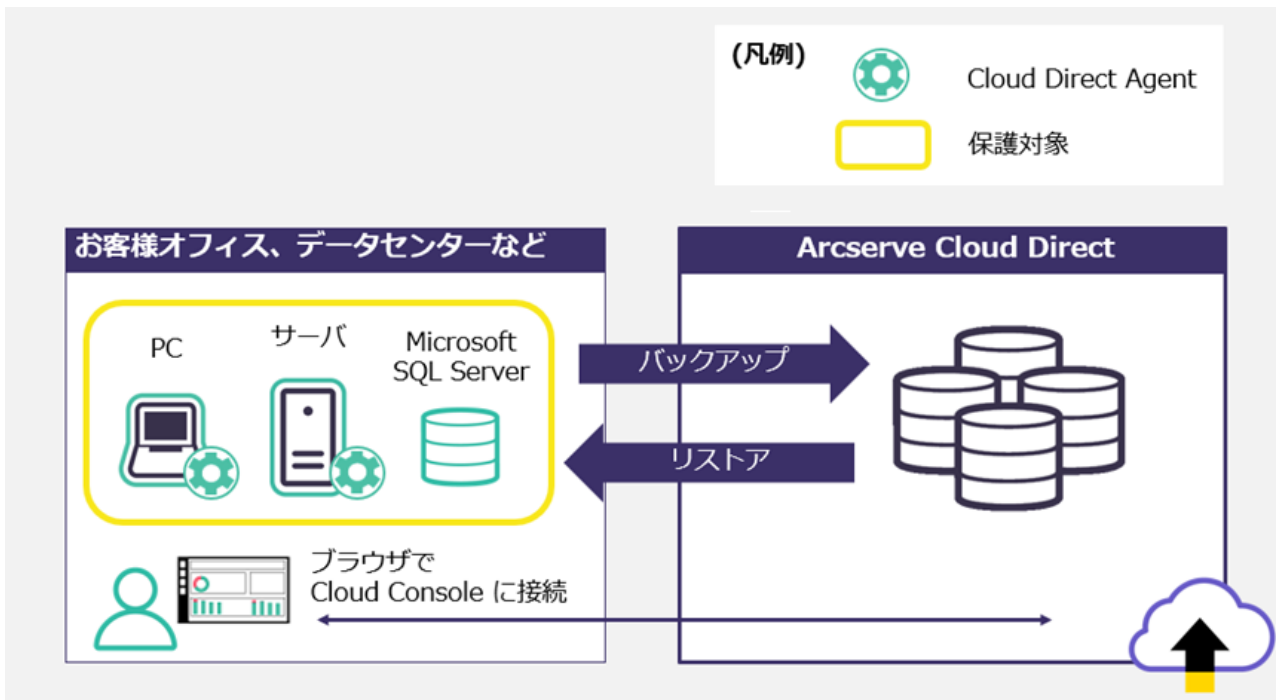
◆ DRaaS 利用時のみ

- VPN サーバ

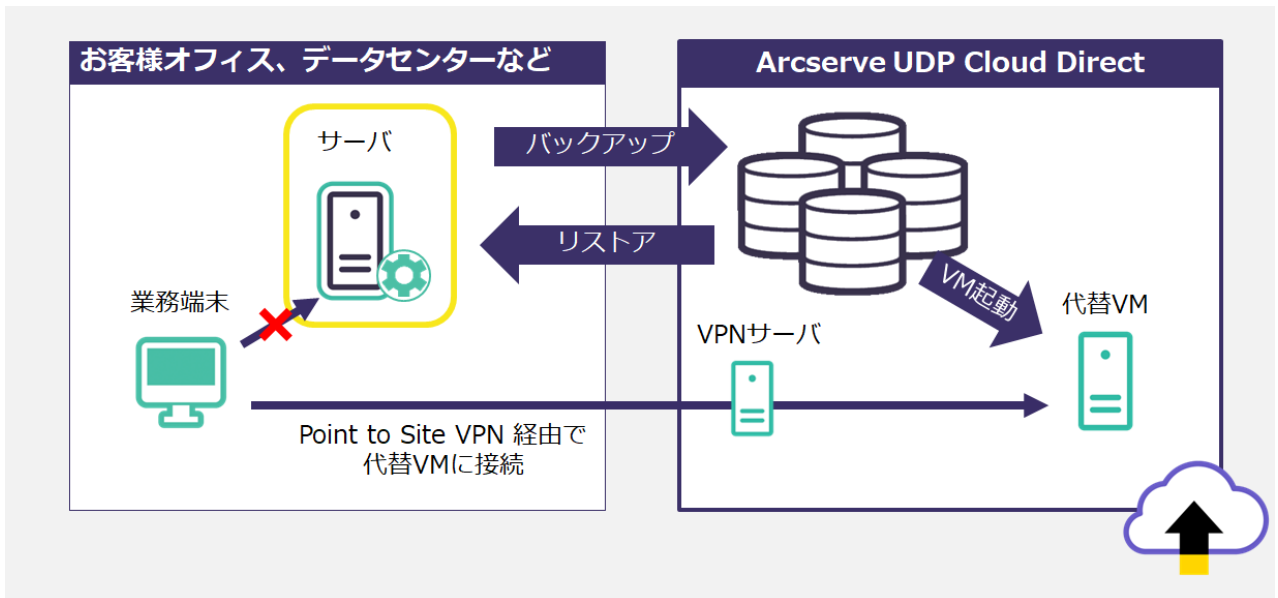
DRaaS の利用時に Arcserve クラウド内に用意されます。オンプレミスから Arcserve クラウドにポイント対サイトの VPN 接続を行う際に使用します。

1.3 Windows 環境のバックアップ構成例

以下は Backup as a Service (BaaS) 構成の一例です。



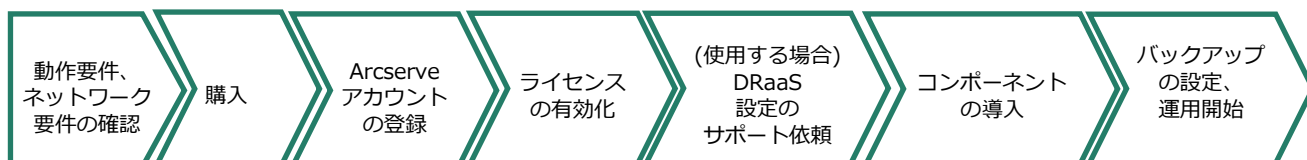
以下は Disaster Recovery as a Service (DRaaS) 構成の一例です。



2 事前確認

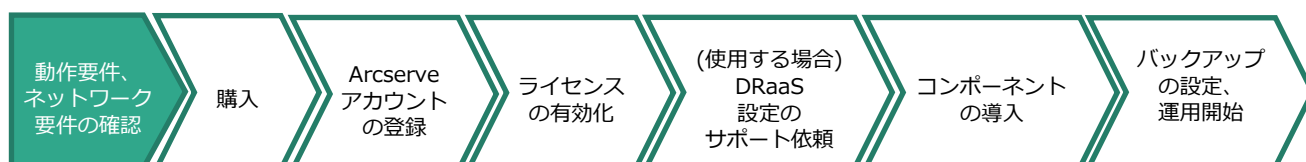
2.1 Arcserve Cloud Direct 環境構築の流れ

この資料では、以下の流れで環境構築の手順を説明します。



2.2 動作要件、その他要件の確認

サブスクリプションの購入前に、保護対象サーバが Arcserve サポート ポータルの動作要件に記載され、ご利用いただくネットワーク環境が要件を満たしていることをご確認ください。



○ 動作要件

<https://support.arcserve.com/s/article/115003836346?language=ja>

○ その他の要件

◆ BaaS/DRaaS 共通

- 各コンポーネントを導入する環境にインターネット接続環境をご用意ください。
- Arcserve Cloud Direct は通信のために以下のポートを利用します。

443/TCP (送信) 、8443/TCP (送信)

お客様環境の Arcserve Cloud Direct Agent がインストールされたサーバから以下のホスト名やサブネットに対して上記ポートで通信できる必要があります。表中で「**使用**」としているポートについては、必要に応じて組織のファイアウォールに送信ポート開放のための設定を行ってください。

Server	443/TCP (送信)	8443/TCP (送信)
admin.zetta.net	使用	不使用

Server	443/TCP (送信)	8443/TCP (送信)
dataapi.zetta.net	使用	不使用
smpping.zetta.net	使用	不使用
smpstatus.zetta.net	使用	不使用
cloud.arcserve.com	使用	不使用
ccapi.arcserve.com	不使用	使用
ccapi-prod1.arcserve.com	不使用	使用
cc1-prod1.arcserve.com	使用	不使用

※接続先に含まれる“zetta”は Cloud Direct の開発部門の旧称です。

以下は、バックアップ先としてご利用になるリージョンに応じて通信を許可してください。

- ・ 210.162.185.0/24 (東日本リージョンの場合)
- ・ 74.114.124.0/22 (Santa-Clara リージョンの場合)

◆ DRaaS 利用時は、以下もご注意ください。

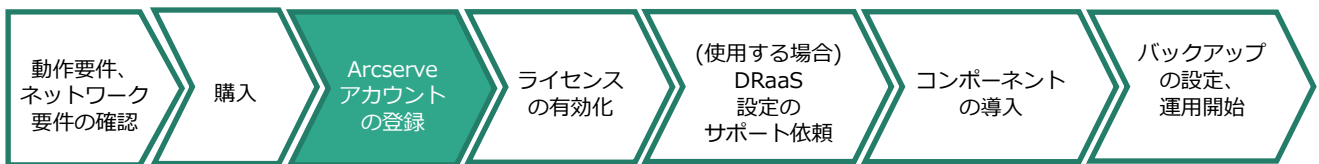
- DRaaS は東日本リージョンでは未提供となります。
- Arcserve テクニカル サポートへの事前お申込みが必要です。詳細は、[3.3 DRaaS 設定のサポート依頼](#)をご覧ください。
- ポイント対サイト VPN の利用のために OpenVPN ツールを使用する時、以下のポート開放が必要です。
 - ・ 1194/UDP (送信/受信)

3 Arcserve アカウントの登録とライセンス有効化

3.1 Arcserve アカウントの登録

サブスクリプションの購入後、Arcserve アカウントをお持ちでない場合は、登録を行ってください。このアカウントは Arcserve の様々なサービスやサポートを利用するための共通アカウントです。

注意：既に他の Arcserve 製品/サービスや Arcserve サポート ポータルのご利用をする際に Arcserve アカウントを作成済みの場合、アカウントは既存のものをご利用ください。

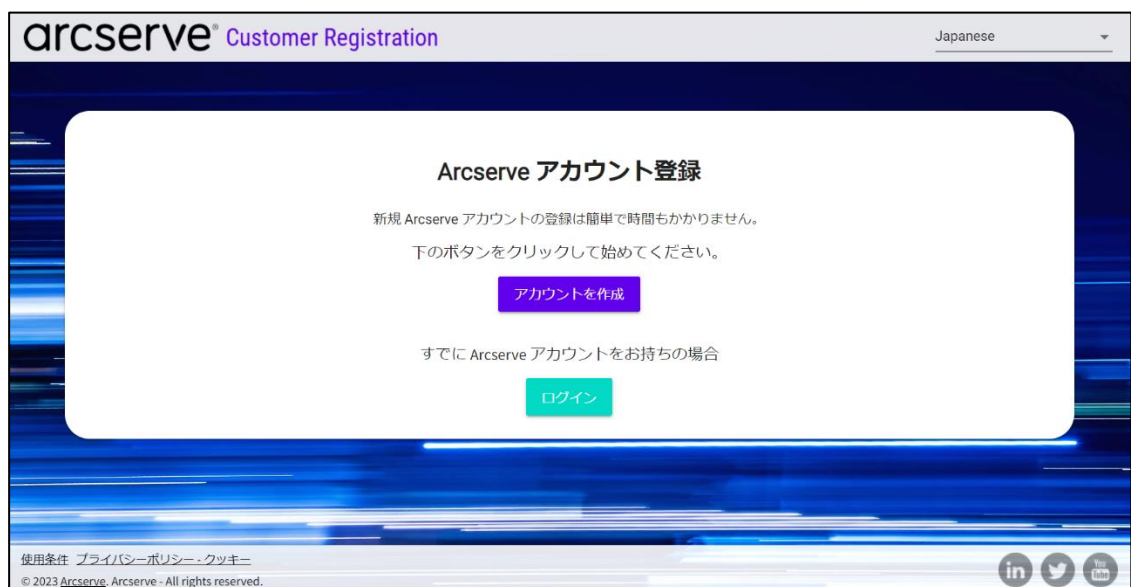


1. Arcserve アカウントをお持ちでない場合は、アカウント作成のために Web ブラウザより以下の URL にアクセスしてください。

<https://registration.arcserve.com/welcome>

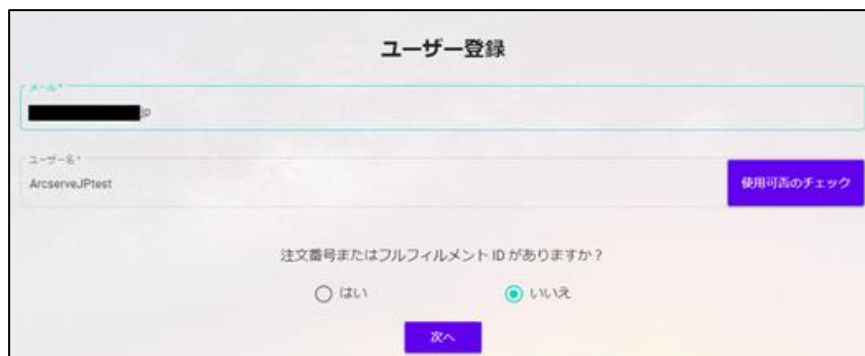
既に Arcserve アカウントをお持ちである場合はこの手順はスキップし、

” 3.2 Cloud Console へのアクセスとライセンスの有効化”に進んでください。

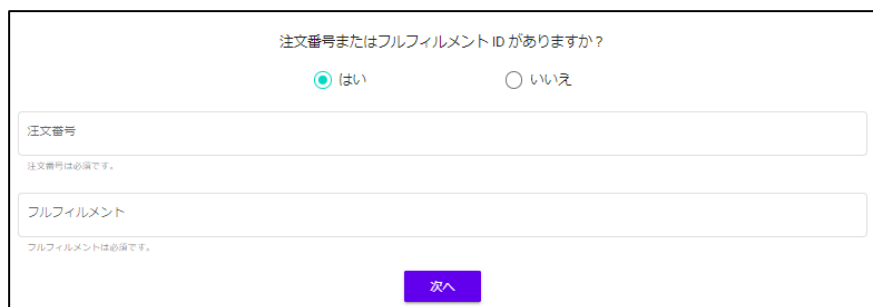


2. [アカウントを作成] をクリックします。

3. 受信可能な電子メールアドレスと、アカウントとして利用するユーザ名を入力します。
[使用可否のチェック]で、ユーザ名が利用可能であることを確認できます。



4. [注文番号またはフルフィルメント ID がありますか?] の質問には、**既にご購入がお済みであったとしても [いいえ] を選択してください。**



5. [次へ] をクリックします。

6. ユーザー詳細として、会社情報とユーザー情報を入力し、[次へ]をクリックします。

ユーザー詳細

以下のArcserveユーザー詳細を入力してください。

会社情報	ユーザー情報
会社名* 株式会社xx	名* Taro
国* Japan	姓* Yamada
都道府県 東京都	ユーザー名 ArcserveJptest
市町村* 千代田区	セカンダリメール [REDACTED]
住所 1* 神保町xxxx	電話* 012-3456-7890
住所 2 神保町三井ビルディングxx階	Japanese
郵便番号 101-0051	

[次へ]をクリックして続行します。

[次へ](#)

登録確認画面が表示されます。

7. 入力した情報を確認し、問題が無ければ[私はロボットではありません]のチェックボックスにチェックを入れ、[今すぐ登録]をクリックします。

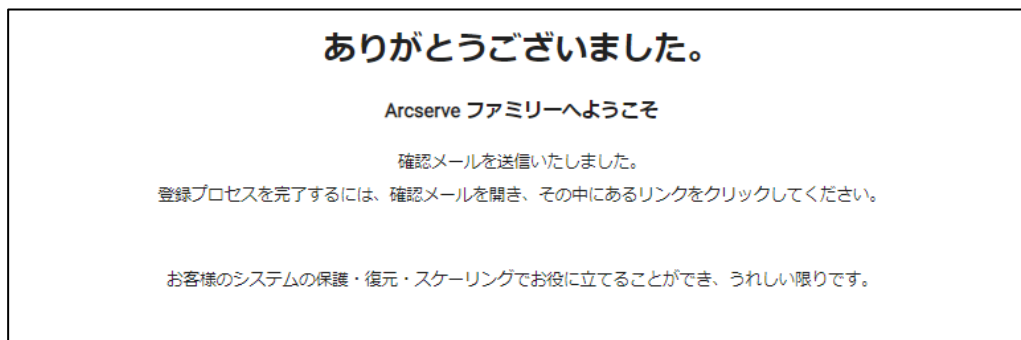
私はロボットではありません

reCAPTCHA
プライバシー・利用規約

ボタンを押して続行してください。

[今すぐ登録](#)

確認メールを送信した旨のメッセージが表示されます。



8. 指定したメールアドレスに HTML メールが届いていることを確認してください。

注意：メールが届かない場合は、no-reply@storagecraft.com からのメールが迷惑メールとしてブロックされていないかをご確認ください。



メール内の [Arcserve アカウントのアクティブ化] をクリックします。

9. ブラウザで Arcserve アカウントの作成が続行されます。

Arcserve アカウントに設定するパスワード、確認のための再入力、パスワードを忘れた場合の質問と回答を入力します。また、任意で SMS でパスワードのリセットまたはアカウントのロック解除を行うための電話番号の追加ができます。

また、セキュリティ画像を選択します。これはフィッシング詐欺を防ぐために、お客様だけがわかる画像を指定していただくことで、偽のログイン画面を見破るための機能です。

設定が完了したら、[マイアカウントを作成する]をクリックします。

Taro さん、Arcserve によろこそ！
Arcserve アカウントを作成する

 新しいパスワードを入力

パスワード要件：

- 8文字以上
- 英字小文字を含む
- 英字大文字を含む
- 数字を含む
- ユーザー名の一部または全部の使用不可

新しいパスワードを再入力

 パスワードを忘れた場合の質問を選択してください

子供の時に一番嫌だった食べ物は何ですか？

回答

 SMS でパスワードのリセットまたはアカウントのロック解除を行うための電話番号を追加 (任意)

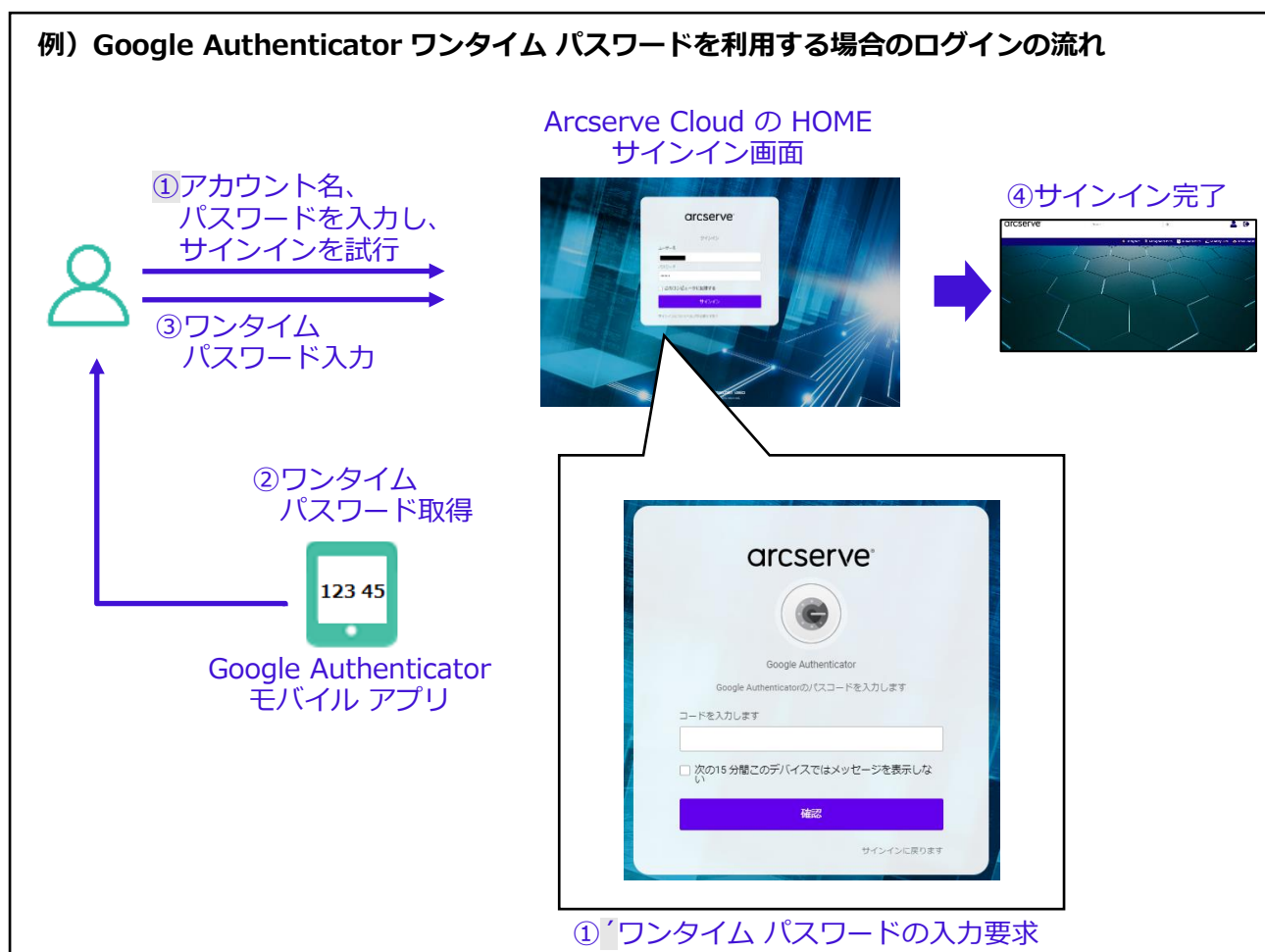
Oktaは、復元コードをテキストメッセージで送信できます。この機能は、メールにアクセスできない場合に便利です。

 画像をクリックして、セキュリティ画像を選択してください

Oktaへのログイン画面に自分だけがわかる画像を設定することで、偽ログイン画面を見破りフィッシング詐欺の被害を防ぐ機能です。

10. Arcserve Cloud の HOME 画面/Cloud Console にサインインするための多要素認証を設定します。Arcserve アカウントのユーザ名、パスワードに加えて、ここで設定した認証方法をクリアすることでサインインが可能となります。



以下の認証方法を利用できます。

- **Okta Verify**

スマートフォンなどのモバイル端末にインストールした「Okta Verify」アプリケーションによりワンタイム パスワードを取得します。

- **セキュリティキーまたは生体認証システム**

セキュリティキー（USB または Bluetooth）または生体認証（Windows Hello や Touch ID など）を利用します。

- **Google Authenticator**

スマートフォンなどのモバイル端末にインストールした「Google Authenticator」アプリケーションによりワンタイム パスワードを取得します。

- **SMS 認証**

スマートフォンなどのモバイル端末で SMS にてワンタイム パスワードを取得します。

- **ボイスコール認証**

携帯電話を使用し、音声の指示に従って認証していただけます。

- **メール認証**

メール送信された認証コードを使用して認証します。



使用する認証方法の [設定] をクリックします。

ここでは、Google Authenticator の設定方法を解説します。その他の認証方法については以下をご参照ください。

Arcserve アカウントの追加の認証 (多要素認証) 設定方法:

<https://support.arcserve.com/s/article/2023021902?language=ja>

11. 機器のタイプとして「iPhone」もしくは「Android」を選択します。

iPhone の場合は AppStore、Android の場合は Google Play Store から Google Authenticator アプリケーションをダウンロード/インストールします。

[次へ] をクリックします。



12. 画面に QR コードが表示されます。

モバイル端末にインストールした Google Authenticator アプリにて、QR コードをスキャンします。



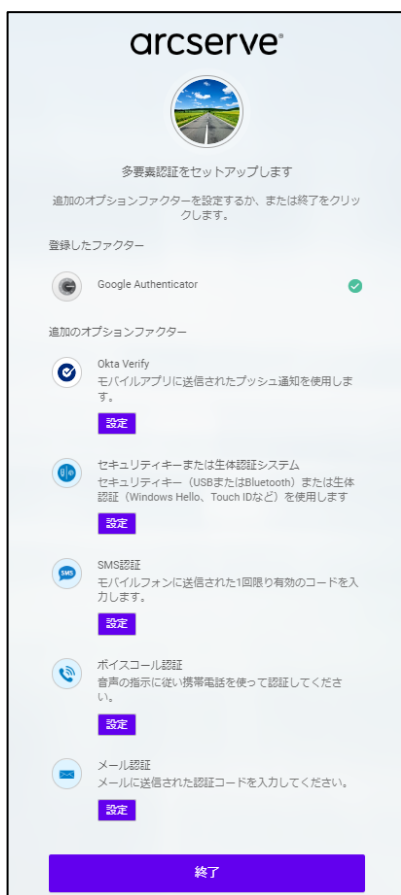
13. Google Authenticator の画面に表示されるコード（ワンタイム パスワード）を入力し、[確認] をクリックします。コードは一定間隔で更新されるため、確認後、すぐに入力する必要があります。



注意：

- モバイル端末の認証システム アプリ上のアカウントは、認証システム アプリの解説をよく読んだうえで、**必ずバックアップを取ってください**。アカウントを設定したモバイル端末の故障/紛失、機種変更、アカウントの誤消去などにより、認証コードの確認ができなくなる場合があります。
- モバイル端末は時刻を正確に合わせてください。
ワンタイム パスワードは、Arcserve の認証システムとモバイル端末、それぞれの環境で時刻を元に生成しています。両者の時刻が一致していないと、生成されるパスワードが食い違うことで認証が通らない場合があります。

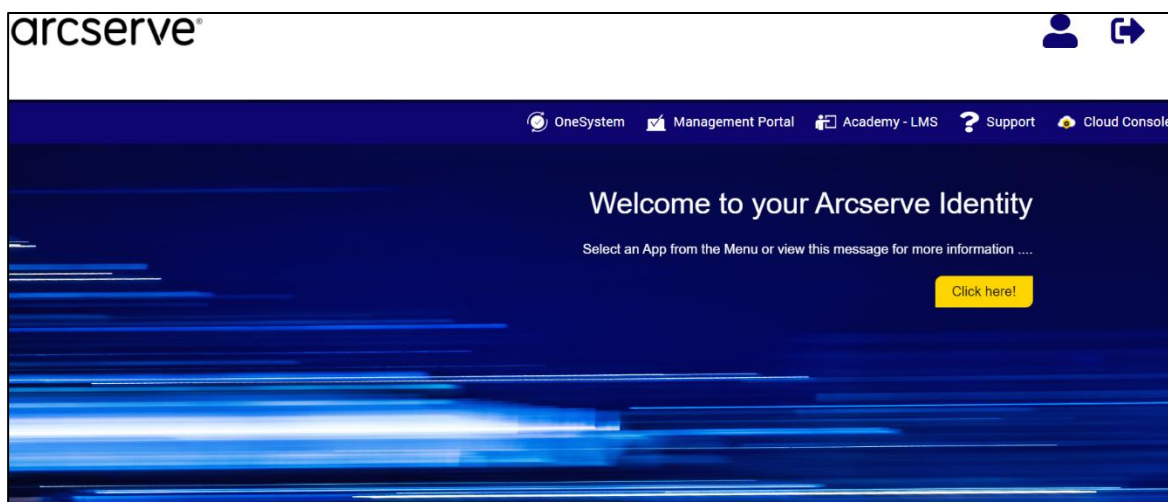
設定が完了し、登録したファクターとして Google Authenticator が表示されます。
追加の認証方法を設定することも可能です。



14. [終了] をクリックします。

これでアカウントの作成は完了です。

Arcserve Cloud の HOME 画面にサインインした状態になります。



3.2 Cloud Console へのアクセスとライセンスの有効化

Cloud Console 上でライセンスの有効化（アクティベーション）を行います。サブスクリプションのご連絡先メールアドレス宛に届くライセンス プログラム証明書をご用意ください。

※メールは送信元が「License-Program (License-Program@arcserve.com)」、件名が「Arcserve - License Order Confirmation #xxxxxxx」（#xxxxxxx は Order ID）となります。



1. ブラウザで以下の URL にアクセスします。

<https://login.arcserve.com/>

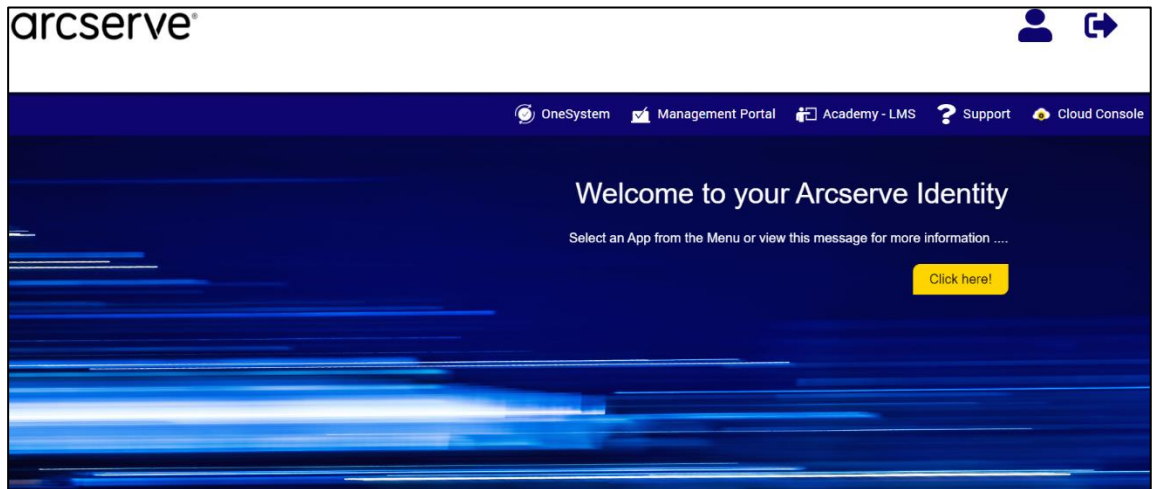
2. サインイン画面が表示された場合、登録済みの Arcserve アカウントのユーザ名、パスワードを入力して、[サインイン]をクリックします。



3. 登録した多要素認証の認証を求められます。一例として、Google Authenticator をご利用の場合は以下の画面にてモバイル アプリで取得したコードを入力し、[確認]をクリックします。



サインインが完了し、Arcserve Cloud の HOME 画面が表示されます。



※こちらのサイトは Arcserve Cloud Direct をはじめ、さまざまな Arcserve 製品を管理するためのポータルとして利用されます。Web ブラウザへのブックマークをお勧めします。

4. Cloud Direct の管理を行うために、[Cloud Console] をクリックします。



Cloud Console の画面と、[アカウントの種類の設定] のポップアップが開きます。



アカウントには以下の2種類があります。

- ・ **エンド ユーザ アカウント**

バックアップやリストアを直接管理するエンド ユーザとして Cloud Direct を利用するアカウントです。

- ・ **2層アカウント**

MSP (Managed Service Provider) として異なるテナントのエンド ユーザにサービスを提供したり、大規模な組織においてドメインやブランチ オフィスを別々に管理する場合などに利用する管理アカウントです。

5. ここでは、エンド ユーザ アカウントを使用した管理方法を解説します。

[エンド ユーザ アカウント] を選択し、[確認] をクリックします。

Cloud Console により Cloud Direct の管理が行える状態になります。



画面上部のアイコンよりさまざまな管理機能が利用できます。



6. 「ダッシュボード」画面にて、画面上部の「保護データ Cloud Direct ボリューム」に [トライアル版の開始] が表示されている場合はクリックしてください。

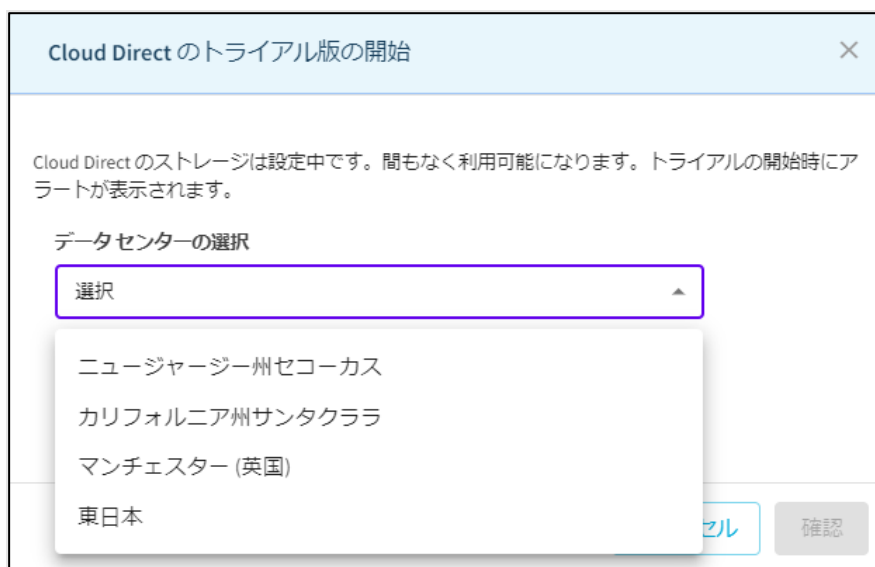


注意：ライセンスをご購入いただいている場合もこの操作は行ってください。

注意：トライアル期間は **15 日間**です。トライアル終了後も継続してご利用いただく場合は、ライセンスのご購入、アクティブ化の操作が必要です。トライアル終了から **30 日以内**にアクティブ化を行ってください。**30 日以後はクラウド上のボリュームが削除されるため、実運用環境への移行はできなくなります。**

7. [データセンターの選択] のリストをプルダウンし、バックアップ先のデータセンターとして、以下のいずれかから選択してください。**既にご購入済みの場合は、購入したストレージサブスクリプションに対応するものを選択してください。**

- ・「カリフォルニア州サンタクララ」（BaaS、DRaaS 対応）
- ・「東日本」（BaaS のみ対応）



それ以外のデータセンターについては選択しないでください。

データセンターの選択後、[確認]をクリックします。

トライアルが開始されます。



この際、バックアップデータを格納するためのデフォルトの「クラウド ボリューム」も作成されます。

[保護] - [Arcserve Cloud] で確認できます。



8. (ご購入済みの場合) ライセンスをアクティブ化するために、[設定]、[エンタイトルメント] をクリックします。



9. 画面右上の、[新しいオーダーのアクティブ化]をクリックします。

10. ライセンス プログラム証書に記載されている [Order ID]、[Fulfillment Number]を入力し、[アクティブ化]をクリックします。

[オーダーは正常に処理されました]と表示され、ライセンス情報が画面に反映されます。

アカウントのサマリ	
Cloud Direct の資格	
ストレージ容量	DRaaS RAM
1 TB	-
DRaaS vCPU	AD サーバ
-	-
追加のパブリック DRaaS IP*	請求タイプ
-	年間サブスクリプション

登録日が購入ライセンスの開始日当日の場合、ライセンスの反映はサービス開始日のカリフォルニア州 サンタクララ時刻の 0:00 以降となるため日本時間では以下の時刻に反映されます。

- サマータイム期間： 日本時間の 16:00
- サマータイム期間外： 日本時間の 17:00

サブスクリプションの開始日は "ライセンス プログラム証書" PDF に記載されています。

ライセンスソフトウェア：	NACDR000SLJS01S12C Arcserve UDP Cloud Direct- Storage 数量: 1	
	- 1TB- US - Annual Subscription	
コンポーネント名	シリアル番号	登録 ID/キーコード
NACDR000SLJS01S12C Arcserve UDP Cloud Direct- Storage - 1TB- US - Annual Subscription		July 27, 2019 - July 26, 2020
To download software, please click here to get started		

3.3 DRaaS 設定のサポート依頼

DRaaS の利用には Arcserve テクニカル サポートへの事前お申し込みが必要です。お申し込みいただくとご購入いただいているストレージ サイズ範囲内で利用可能な DRaaS 専用ボリュームを追加します。



下記、Arcserve サポート ポータルにて DRaaS の有効化を依頼します。

Arcserve サポート ポータル : <https://support.arcserve.com/s/?language=ja>

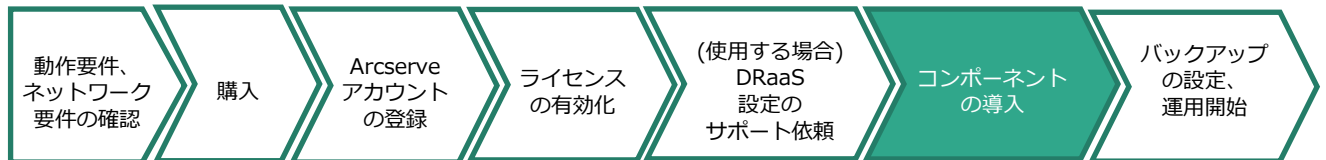
サポートポータルの利用方法については以下 URL のポータルマニュアルをご覧ください。

<https://support.arcserve.com/s/article/202937699?language=ja>

4 コンポーネントの導入

4.1 必要なコンポーネントのダウンロード

Windows 環境のバックアップに必要な Cloud Direct エージェントをダウンロードします。



1. Cloud Console にログインし、画面上部のアイコンから[サポート]を選択し、[ダウンロード] - [リリースの表示]をクリックします。



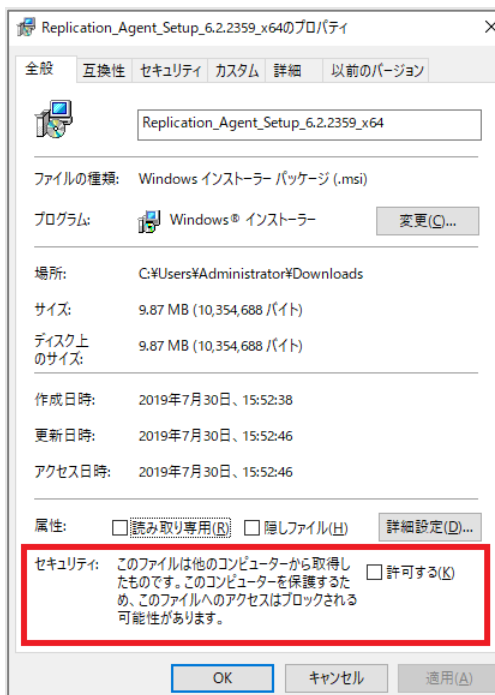
2. 導入する OS 環境に合致するエージェントの [ダウンロード] リンクをクリックします。

Cloud Direct の場合 登録認証情報の表示					
Windows					
リリース名	バージョン詳細	リリース日	リリースノート	インストールガイド	
Cloud Direct Agent 6.2 (64)	6.2	2020/7/28	リリースノートの表示	ガイドの表示	↓ ダウンロード
Cloud Direct Agent 6.2 (32)	6.2	2020/7/28	リリースノートの表示	ガイドの表示	↓ ダウンロード
Linux					
リリース名	バージョン詳細	リリース日	リリースノート	インストールガイド	
VMware Appliance 6.2 (64)	6.2	2020/7/28	リリースノートの表示	ガイドの表示	↓ ダウンロード
Cloud Direct Agent 6.2 (32)	6.2	2020/7/28	リリースノートの表示	ガイドの表示	↓ ダウンロード

ブラウザのダウンロード フォルダにエージェントがダウンロードされます。

4.2 Windows 用 Agent のインストール

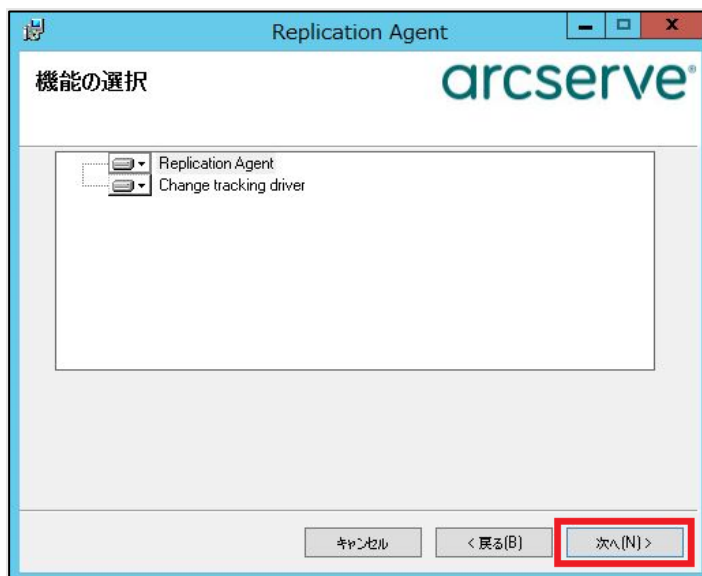
1. 保護対象マシンに管理者権限を持つアカウントでログインし、インターネットに接続できることを確認して、ダウンロードされたインストーラ ファイルを実行します。Windows によって PC が保護された旨のメッセージが表示された場合は、インストーラ ファイルを右クリックし、プロパティをクリックします。他のコンピュータから取得したファイルの実行のブロックを解除するために、セキュリティの設定で「許可する」にチェックを入れて[OK]をクリックします。



2. セットアップ ウィザードが起動します。[次へ] をクリックします。



3. 機能がすべて選択されていることを確認し、そのまま [次へ] をクリックします。

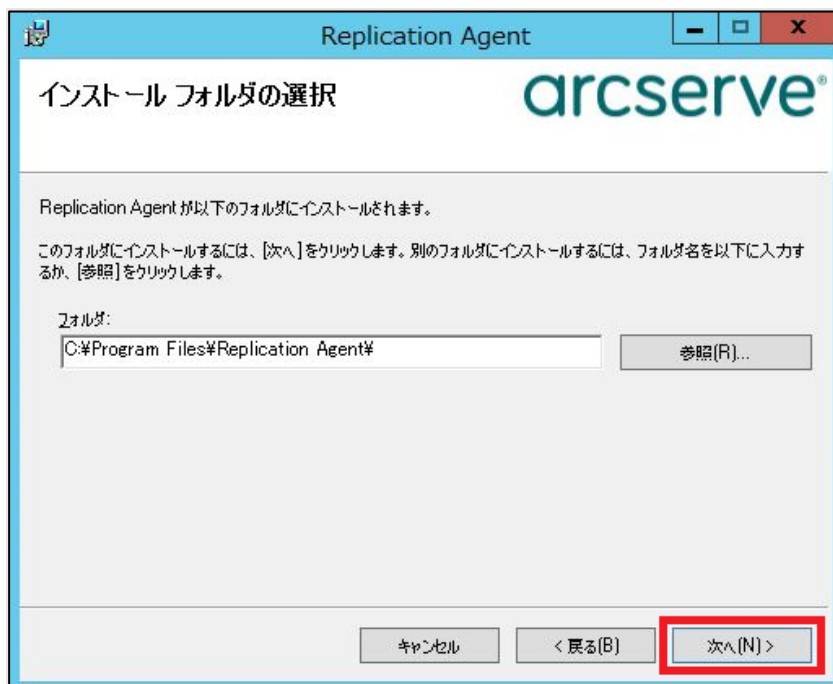


注意 : Arcserve UDP のエージェントがインストールされている環境では、"Change tracking driver" についてはインストールを行わないでください。詳細は下記サイトの「5. DRaaS は Arcserve UDP によるエージェントベース Windows バックアップと併用することはできません。」および「6. BaaS は Arcserve UDP との併用が可能です。Arcserve Cloud Direct (BaaS) は、Arcserve UDP の変更ブロック トラッキング ドライバは使用しません。」をご参照ください。

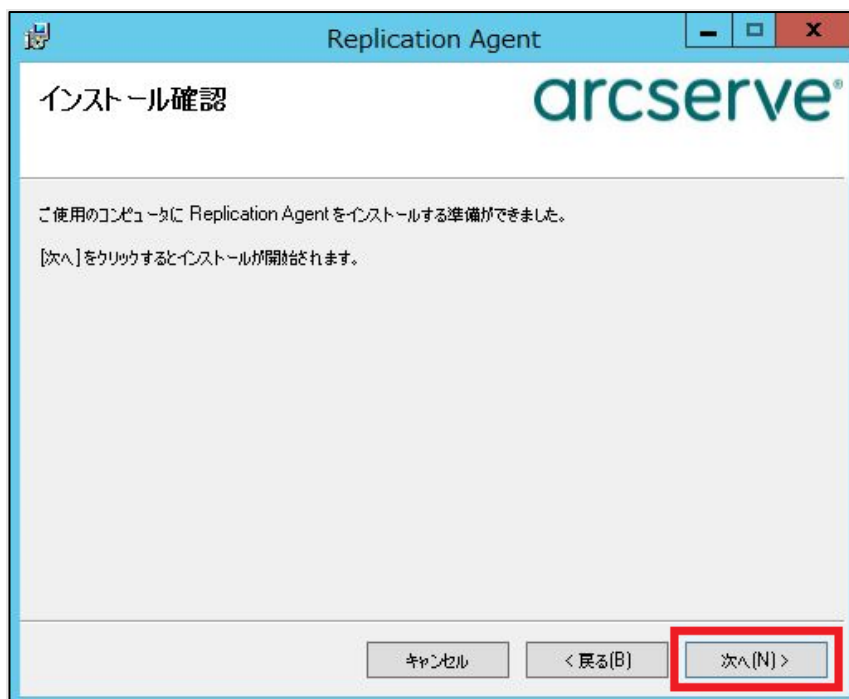
注意/制限事項

<https://support.arcserve.com/s/article/2019081401?language=ja>

4. インストール先フォルダを確認し、[次へ] をクリックします。



5. インストールを開始するため、[次へ] をクリックします。



6. 正常にインストールされたことを確認し、[閉じる]をクリックします。



注意：お客様の環境でインターネット接続のためにプロキシ設定が必要な場合は、Windows のタスクトレイで Arcserve Cloud Direct のエージェント アイコンを右クリックし、[ローカル設定]をクリックします。



[プロキシを使用]にチェックを入れ、プロキシ サーバ及びポートを指定します。認証が必要な場合は、下の[アカウント]にチェックを入れてアカウント情報を入力し、[OK] をクリックします。



注意：

ここでの設定は Arcserve Cloud Direct のサービスを実行するアカウントや、CIFS 共有フォルダをバックアップする際のアクセス アカウントとしても利用されます。

7. Cloud Console にバックアップ対象の情報を登録するためのポップアップが表示されます。

システム名としては、Cloud Console 上でこのシステムを固有に認識するための、ホスト名（フレンドリ名）が自動入力されますが、任意の名前に変更可能です。

「ユーザ名」、「パスワード」に入力する内容については、

Cloud Direct のエージェントのダウンロード ページ（Cloud Console 画面上部のアイコンから[サポート]を選択し、[ダウンロード] - [リリースの表示]）にて確認します。

「Cloud Direct の場合」の隣、「登録認証情報の表示」リンクをクリックします。

リリース名	バージョン詳細
Cloud Direct Agent 6.2 (64)	6.2
Cloud Direct Agent 6.2 (32)	6.2

これにより、エージェントを登録する際に必要なユーザ名、パスワードを確認することができます。

ユーザ名、パスワードを入力完了後、[サイン イン]をクリックします。

Cloud Console で、[保護] - [ソース] の一覧に指定ノードが登録されたことを確認します。

Cloud Console で[保護] - [ソース] の一覧に指定ノードが登録されたことを確認します。



5 バックアップの設定



5.1 バックアップ先ボリュームの作成

デフォルトでは BaaS 用のボリュームが 1 つ作成済みですが、このボリューム名は変更できないので、任意の名前を持つボリューム名をバックアップ先として利用する場合はボリュームを新規に作成します。この資料では、新しいボリュームを作成する手順を説明します。

※BaaS 用のボリュームは Cloud Console で作成できます。DRaaS 用ボリュームは Arcserve テクニカルサポートへ作成を依頼してください。詳細は「[3.3 DRaaS 設定のサポート依頼](#)」をご参照ください。

1. Cloud Console において、[保護] – [Arcserve Cloud]を開き、右上の [クラウド ボリュームの追加] をクリックします。



2. クラウド ボリュームの追加画面が表示されます。コメント以外のすべての情報を入力すると [クラウド ボリュームの追加] を押し、ボリューム追加ができるようになります。

- ・ボリューム名 ※作成するボリュームに任意の名前を入力してください。
- ・データセンター ※[カリフォルニア州サンタクララ] もしくは [東日本] のうち、購入したストレージサブスクリプションに対応するものを選択してください。
- ・コメント ※任意のコメントです。
- ・保存 ※ここで指定した期間、バックアップデータは Arcserve クラウド上に保持されます。BaaS 用ボリュームでは 7 日、14 日、1 か月、2 か月、3 か月、6 か月、1 年、2 年、3 年、7 年、10 年、無期限から選択できます。DRaaS 用ボリューム（Arcserve テクニカル サポート経由で作成）は 7 日、14 日、1 か月から選択となります。

ニュージャージー州セコーカス

カリフォルニア州サンタクララ

マンチェスター (英国)

東日本

クラウドボリュームの追加 ×

アカウント名
Arcserve Cloud Direct

データセンター
東日本

保存
7日

時間単位で保存: 0 時間
月単位で保存: 0 月

ボリューム名①
EastJapan1

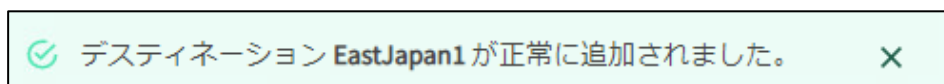
コメント
オプション

週単位で保存: 0 週
日単位で保存: 7 日
年単位で保存: 0 年

4時間単位で保存: 0 interval (0 days)

キャンセル
クラウドボリュームの追加

3. Cloud Console 上のポップアップから、ボリュームが作成されたことを確認できます。



5.2 ポリシー作成の開始

Arcserve Cloud Direct ではバックアップの設定を「ポリシー」として作成し、これをバックアップ対象マシンに割り当てることでバックアップを行ないます。

デフォルトではコンピュータ全体をバックアップするポリシーが1つ作成済みです。

名称を変更して利用することも、新しいポリシーを作成することもできます。

今回は、新しいポリシーを作成する手順を確認します。

1. Cloud Console において、[保護] - [ポリシー]の順にクリックし、画面右上、[ポリシーの追加] をクリックします。



5.3 基本情報の設定

[基本情報] タブが自動的に選択されるので、[ポリシー名] を入力し、[保護タイプ]を指定すると、[ソース(オプション)] タブ、[タスク] タブの設定に進むことができます。



[基本情報]タブ設定には、以下の項目を設定します。

- ・ポリシー名 ※ ポリシー名を入力します。入力必須です。
- ・保護タイプ ※ 入力必須です。
 - Arcserve Cloud へのエージェント ベースの直接バックアップ ※ BaaS タイプの保護をおこないます。
 - 惨事復旧のための Arcserve Cloud へのエージェント ベースのバックアップ ※ DRaaS タイプの保護を行います。
- ・説明 (オプション) ※ 任意の説明を入力できます。

5.4 ソースの設定

- [ソース(オプション)]タブをクリックします。画面右上の[ソースの選択]をクリックすると、ノードリストが表示されます。



- 表示されたリストから保護対象マシンの左横のチェックボックスにチェックを入れ、右上の[ソースの追加] ボタンをクリックすることで、ポリシーがマシンに割り当たります。

※ ノードへのポリシーの割り当ては、ポリシー作成後に行うことも可能です。



5.5 タスクの設定

[タスク] タブをクリックします。ここでは、以下の4つの詳細タブで保護対象や保護する場所（バックアップ先）、タイミング（スケジュール）などの設定を行います。

- [1. 保護対象]
- [2. 保護する場所]
- [3. 保護するタイミング]
- [追加の設定] ※ 保護対象に[Cloud Direct ファイル フォルダ バックアップ]を選択した場合のみ



5.5.1. 保護対象の設定

[1. 保護対象] タブでは、[アクティビティのタイプ] を選択します。

※[基本情報] タブで選択した保護タイプにより選択肢が異なります。



アクティビティのタイプには以下があります。

※[Exchange] については日本では未サポートとなります。

- **[Windows イメージ (ディスク ドライブ全体)] ※BaaS/DRaaS で選択可**

システム全体もしくはディスク全体のイメージ バックアップを行います。

初回のバックアップ時には未使用領域を含めたディスク全体に対して読み込み処理が行われるので、その分の時間がかかることにご注意ください。

例えば 100 GB バイト容量のバックアップ対象ディスクに 30 GB のデータが格納されている場合、初回のバックアップでは 100 GB 分に対して読み込みが行われます。

ただし、Cloud Direct ストレージには、30 GB 分のバックアップが保存されます。

また、BaaS 用ボリュームへの Windows イメージ バックアップでは、増分バックアップ時にファイルのタイムスタンプに変更があったファイルを確認した上で、該当ファイルの変更ブロックを抽出してバックアップを行うという、2 段階の処理が行われます。そのため、バックアップされる容量は小さくなるものの、増分バックアップ時間はフルバックアップより長くなる場合があります。

[すべてのボリュームのバックアップ] を選択した場合、システム上に存在するすべてのドライブがバックアップされます。[選択したボリュームのバックアップ] を選択した場合、任意のドライブのバックアップができます。バックアップしたいドライブ文字のチェック ボックスを選択してください。

※ DRaaS により Arcserve クラウドに復旧を行うためには、システム ドライブとブート ボリュームを保護対象に含めてください。

※ Cloud Direct には BMR (ベアメタル復旧) 機能はありません。

- **[Cloud Direct ファイル フォルダ バックアップ]** ※Baasのみ選択可

特定のフォルダを指定してバックアップを行います。

バックアップしたいフォルダへのフルパスを入力してください。



詳細 | 1. 保護対象 | 2. 保護する場所 | 3. 保護するタイミング | 追加の設定

アクティビティのタイプ

Cloud Direct ファイル フォルダ バックアップ ⓘ

パス | 追加

D:\ImportantData

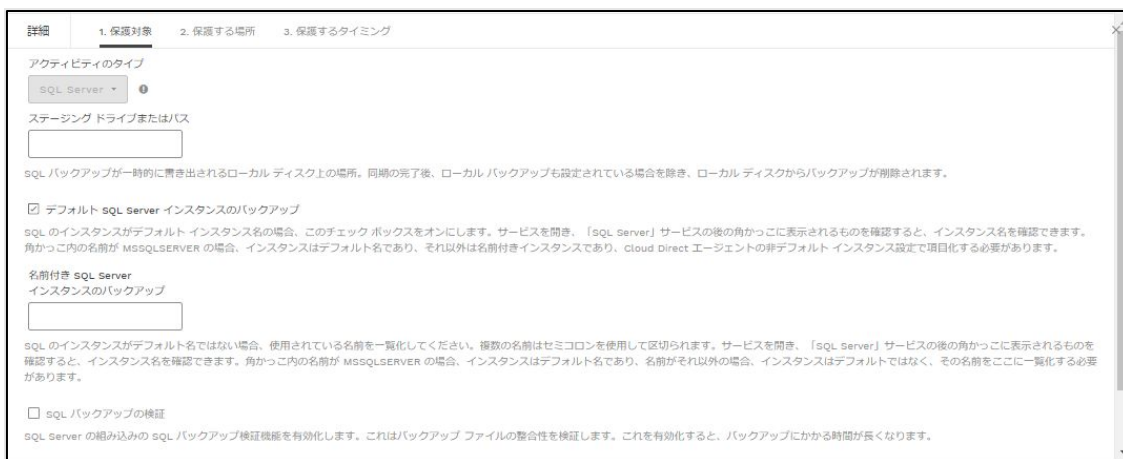
UNC パス (¥¥サーバ名¥共有名) を指定することで、NAS や共有フォルダ上のデータのバックアップも可能です。※その場合はエージェントのアイコンから、[ローカル設定]画面を開き、共有にアクセスするためのアカウント情報を指定してください。

複数のフォルダをバックアップする場合は、[追加] ボタンによりパス フィールド行を追加できます。

- **[SQL Server]** ※BaaSのみ選択可

Microsoft SQL Server のデータをオンラインでバックアップしたい時に使用します。

SQL Server をバックアップする際には、一次バックアップとしてローカル ディスクにバックアップを行い、その後 Arcserve クラウドにバックアップを行うという、2 段階 (“ステージング”方式) での処理となります。



詳細 | 1. 保護対象 | 2. 保護する場所 | 3. 保護するタイミング

アクティビティのタイプ

SQL Server ⓘ

ステージング ドライブまたはパス

SQL バックアップが一時的に書き出されるローカル ディスク上の場所。同期の完了後、ローカル バックアップも設定されている場合を除き、ローカル ディスクからバックアップが削除されます。

デフォルト SQL Server インスタンスのバックアップ

SQL のインスタンスがデフォルト インスタンス名の場合、このチェック ボックスをオンにします。サービスを開き、「SQL Server」サービスの後の角かっこに表示されるものを確認すると、インスタンス名を確認できます。角かっこ内の名前が MSSQLSERVER の場合、インスタンスはデフォルト名であり、それ以外は名前付きインスタンスであり、Cloud Direct エージェントの非デフォルト インスタンス設定で項目化する必要があります。

名前付き SQL Server インスタンスのバックアップ

SQL のインスタンスがデフォルト名ではない場合、使用されている名前を一覧化してください。複数の名前はセミコロンを使用して区切られます。サービスを開き、「SQL Server」サービスの後の角かっこに表示されるものを確認すると、インスタンス名を確認できます。角かっこ内の名前が MSSQLSERVER の場合、インスタンスはデフォルト名であり、名前がそれ以外の場合、インスタンスはデフォルトではなく、その名前をここに一覧化する必要があります。

SQL バックアップの検証

SQL Server の組み込みの SQL バックアップ検証機能を有効化します。これはバックアップ ファイルの整合性を検証します。これを有効化すると、バックアップにかかる時間が長くなります。

[ステージング ドライブまたはパス]に、一次バックアップ先となるドライブ、もしくはパスを指定します。

デフォルトでは既定のインスタンス (MSSQLSERVER) をバックアップします。

既定のインスタンスのバックアップが不要な場合は [デフォルト SQL Server インスタンスのバックアップ] のチェックを外してください。

インスタンス 名を指定してバックアップする場合は [名前付き SQL Server] にバックアップ対象のインスタンス名を入力します。複数のインスタンス名を入力する場合は、';' (セミコロン) で区切って入力をしてください。

※SQL Server のインスタンス名は、Windows のサービス画面で確認できます。“SQL Server (インスタンス名)” サービスの括弧内の文字列がインスタンス名です。

[SQL バックアップの検証] にチェックを入れることで、SQL Server の機能を利用して SQL バックアップ データの整合性を検証することができます。

<参考 : アクティビティのタイプとリストア単位>

バックアップの取り方により、リストアできる単位が異なります。

	バックアップ単位	リストア単位 (お客様サイトへのリストア)	プロビジョニング単位 (Arcserve クラウドでの VM 起動)
BaaS	Windows イメージ (すべてのボリューム/ 選択したボリューム)	ディスク イメージ ※1、ファイル、フォルダ	-
	ファイル フォルダ	ファイル、フォルダ	-
	SQL Server	データ ファイル、ログ ファイル ※2	-
DRaaS	Windows イメージ (すべてのボリューム/ 選択したボリューム)	ディスク イメージ、ファイル、フォルダ	Windows イメージ (バックアップしてあるボリュームのみ)

※1 ディスク イメージは、img、vhdx 形式となります。img 形式のファイルは Raw Disk Image 対応のツールでディスクとしてマウントできます。vhdx ファイルは Windows Server 2012 以降で、マウントできます。

ただし、いずれの形式のファイルもブート ボリュームとしてマウントする事はサポートされません。

※2 SQL Server のバックアップデータはリストア時に bak 形式のファイルとなります。リストア後に SQL Server の機能でデータベースとして利用できるように復元できます。データベースの復元手順の詳細はマイクロソフト社の情報をご参照ください。

5.5.2. 保護する場所の設定

[2. 保護する場所] タブを開き、バックアップ先となる Arcserve クラウド上のボリュームを指定します。

[デスティネーション] 下の [選択] ボタンをクリックし、プルダウンメニューから作成済みのクラウド ボリュームを選択します。

[ローカル バックアップを作成する] にチェックを入れると、Arcserve クラウドへのバックアップとは別に、ローカル ディスク上にバックアップデータを残すことができます。ローカル バックアップを行なう場合は [ローカル バックアップ パス] に格納先フォルダのパスを指定してください。

注意 : ローカル バックアップではバックアップ方式として [Windows イメージ (ディスク ドライブ全体)] を選択した、ローカルディスクにフル バックアップと同等サイズのテンポラリーデータが作成されます。そのため、フル バックアップ 2 回分以上の空き領域を持つドライブをローカル バックアップの作成先として指定してください。

5.5.3. 保護するタイミングの設定

[3. 保護するタイミング] タブを開き、バックアップ スケジュールを設定します。

バックアップスケジュール間隔は BaaS では[1 日ごと] で固定です。

DRaaS では「15 分ごと」、「1 時間ごと」、「6 時間ごと」、「1 日ごと」のいずれかを指定できます。

注意：DRaaS のデフォルトでは「15 分ごと」が選択されています。必要に応じ変更してください。

[開始時刻]には最初にバックアップを実行するタイミングを指定してください。

[バックアップ スケジュール]では実行する曜日を指定できます。青い色がついている曜日にはバックアップが実行されます。クリックで変更できます。

スロットル スケジュールで [追加] をクリックすると、帯域制御設定が追加できます。例えば、平日日中のバックアップによるインターネット使用量を制限し業務への影響を抑えたい、という場合に設定してください。

[スループット制限]では、各ポリシーがバックアップに使用できる帯域幅の上限値を設定します。

[実行予定日]では、帯域制御を行なう曜日を指定します。

[開始時刻]と[終了時刻] で帯域制御を行なう時間帯を指定します。

5.5.4. 追加の設定

[キャッシュの場所]で転送を効率化するためのローカル キャッシュの保存場所を指定できます。バックアップデータの1%程度の領域が必要です。

[バックアップ前のスクリプト][バックアップ後のスクリプト]では、バックアップの前後に任意のスクリプトを実行するように指定できます。（ファイル/フォルダ バックアップ時のみ）

[除外ルール]でバックアップ対象から任意のファイルやディレクトリを除外するための設定が行えます。[除外ルール] の下の [選択] を開き、ルールを追加します。

「ファイル」、「ディレクトリ」では、[値] 欄に入力した名前が一致したファイルやディレクトリを全てバックアップ対象から除外します。「パス」では、入力したパスが一致したファイルやフォルダのみをバックアップ対象から除外します。

※ 1文字以上の任意の文字を置き換えるワイルドカード (*) も使用可能です。

5.6 ポリシー設定の完了

[ポリシーの作成] をクリックして設定を保存します。

これでバックアップの設定は完了です。

ポリシーで設定したスケジュールに基づき、バックアップが実行されます。

5.7 バックアップ結果の確認

バックアップの進捗や実行結果は [レポート]-[ジョブ]をクリックし、確認したいジョブ名をクリックすることで確認できます（進捗状況は表示されるまで時間がかかる場合があります）。

アクション	ソース	ジョブ名	ジョブタイプ	ステータス	ポリシー
<input type="checkbox"/>	CDTEST4	CDTEST4 から EastJapan1 へバックアップ	バックアップ - 増分	処理中 (33% 完了)	TEST POLICY
<input type="checkbox"/>	CDTEST4	CDTEST4 から EastJapan1 へバックアップ	バックアップ - フル	完了	TEST POLICY
<input type="checkbox"/>	CDTEST4	CDTEST4 のポリシー展開	ポリシー展開	完了	TEST POLICY

一般		
進捗状況 33% 完了	開始時刻 2020年12月4日 16:33	経過時間 3 分 51 秒
エラー カウント 0	警告カウント 0	重大度 正常に展開されました
ステータス ● 処理中		
スループット		
処理済みサイズ 5.65 GB	変更された処理済みサイズ 5.65 GB	処理済みファイル 0
未圧縮転送 520.67 MB		

5.8 タスクの追加、変更、削除

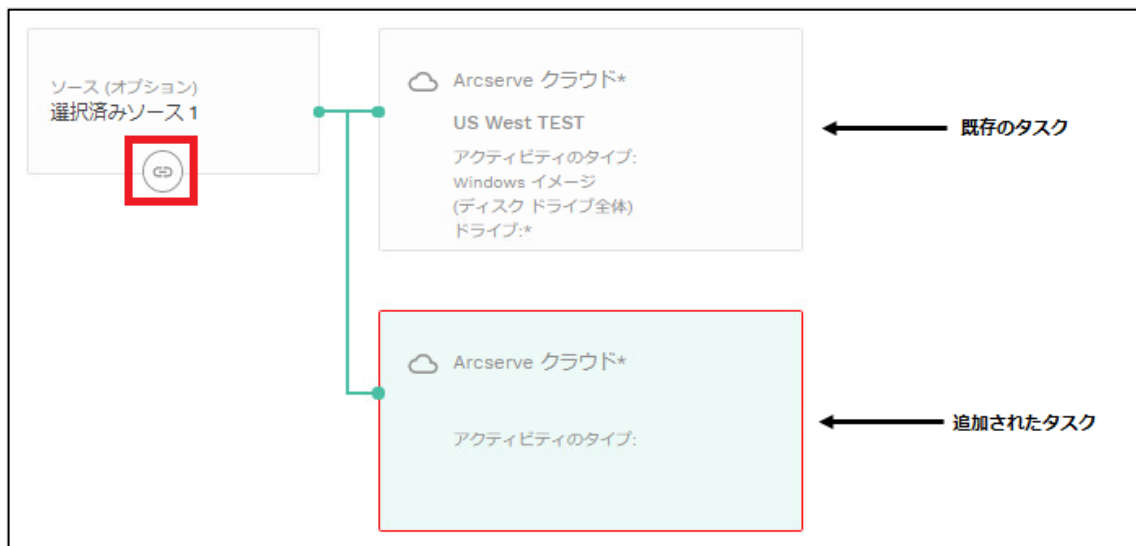
ポリシーの [タスク] タブでは画面上部にタスクの構成が図示されます。

ポリシー画面上ではタスクの変更と追加が可能です。



5.8.1. タスクの追加方法

ソース (オプション) の下のアイコンをクリックすることで、タスクを追加することができます。



例えば、1つのマシンでディスク全体のバックアップと SQL Server のオンライン バックアップを併用したい時はデスティネーションを追加することで実現できます。

また、1台のサーバの複数ドライブに対して、ドライブごとに Windows イメージのバックアップタスクと、ファイル/フォルダ 単位のバックアップ タスクといった異なるバックアップ方式を割り当てて使用することも可能です。

5.8.2. タスクの削除方法

既存のタスクを選択しているときに画面下部の[デスティネーションの削除]をクリックすることで、タスクを削除できます。



6 データのリストア

6.1 フォルダのリストア

ここでは、ディスク イメージのバックアップから、特定のフォルダをリストアする例を説明します。

1. [保護] - [ソース]をクリックします。



2. リストアしたいマシン名のリンクをクリックします。



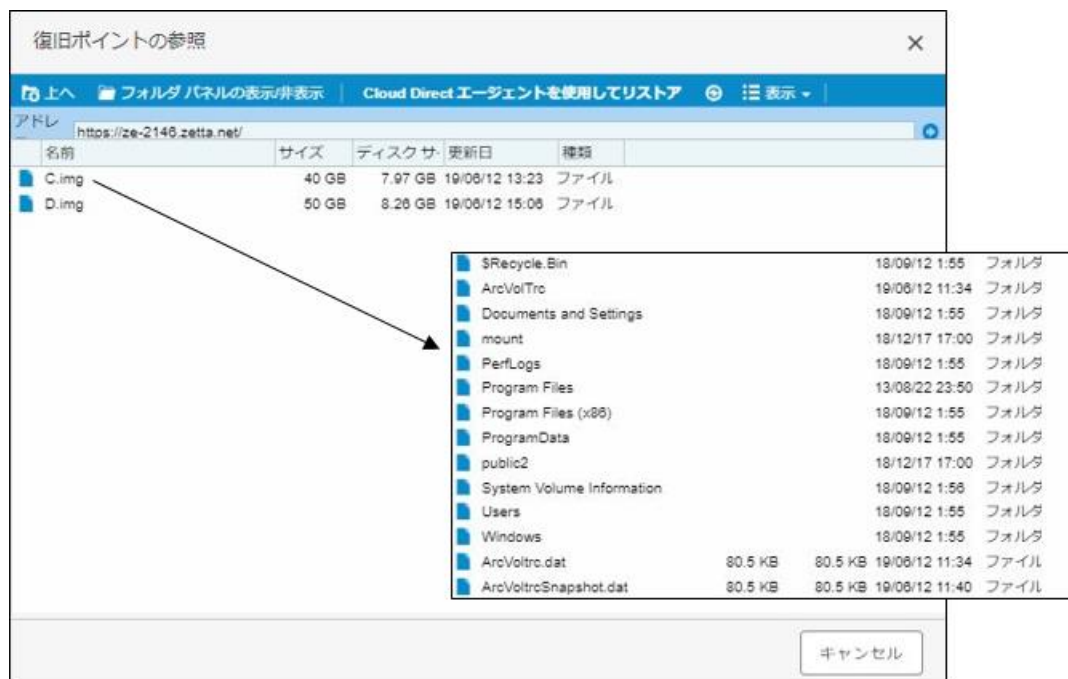
3. [復旧ポイント]タブをクリックすると、復旧ポイントがドライブ単位でリスト表示されます。リストアしたい復旧ポイントの [アクション] カラムでプルダウンから [復旧] をクリックします。



4. 特定のフォルダをリストアするためには、[復旧ポイントの参照]をクリックします。



5. リストアしたいフォルダやファイルをブラウズできます。



6. リストア対象フォルダを右クリックして[Cloud Direct エージェントを使用してフォルダをリストア]をクリックします。



7. 復旧元とデスティネーションパスを確認し、右下の [次へ] をクリックします。

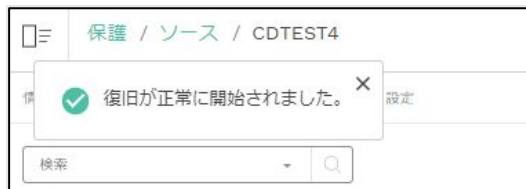


8. [元のソース マシンに復旧]を選択するとバックアップ元のマシンにリストアします。[別のマシンに復旧]を選択した場合は、リストからリストア先マシンを指定します。

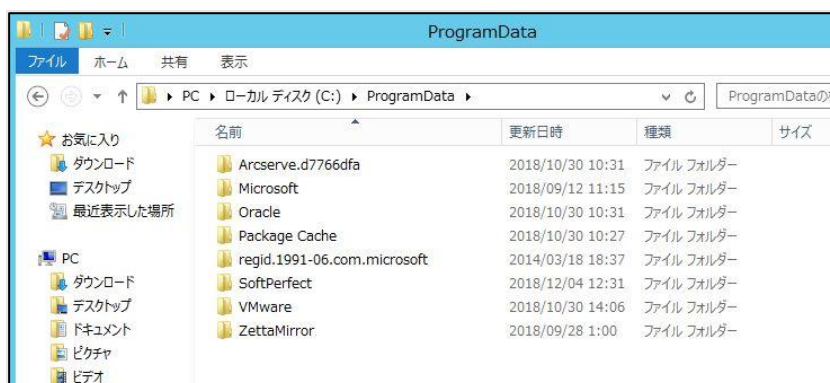
右下の [リストア] をクリックし、リストアを開始します。



9. リストアの開始がポップアップメッセージで表示されます。



10. リストア結果はログで確認できます。リストアしたフォルダを開き、正常に復旧が完了したことを確認してください。



6.2 イメージのリストア

ディスク全体をバックアップしていた場合、ボリュームのイメージ単位でリストアすることも出来ます。以下の図のようにイメージのフォーマットを指定できます。

The screenshot shows a restore configuration window. At the top, the source path is "/ZettaMirror/zsystem44/VOLUME/D.img" with a link for "復旧ポイントの参照". Below this, there are three main sections: "イメージフォーマット" (Image Format), "デスティネーションパス" (Destination Path), and "出力ファイル名" (Output File Name). The "イメージフォーマット" section has a dropdown menu with "選択" (Select) and a downward arrow, and two options: "img" and "vhdx". The "デスティネーションパス" section has a text input field containing "C:\". The "出力ファイル名" section has a text input field containing "D.img". Red boxes highlight the dropdown menu and the destination path field.

イメージフォーマット	デスティネーションパス	出力ファイル名
選択 ▼ img vhdx	C:\	D.img

7 Arcserve クラウドに復旧された VM へのアクセス

7.1 プロビジョニングの実施

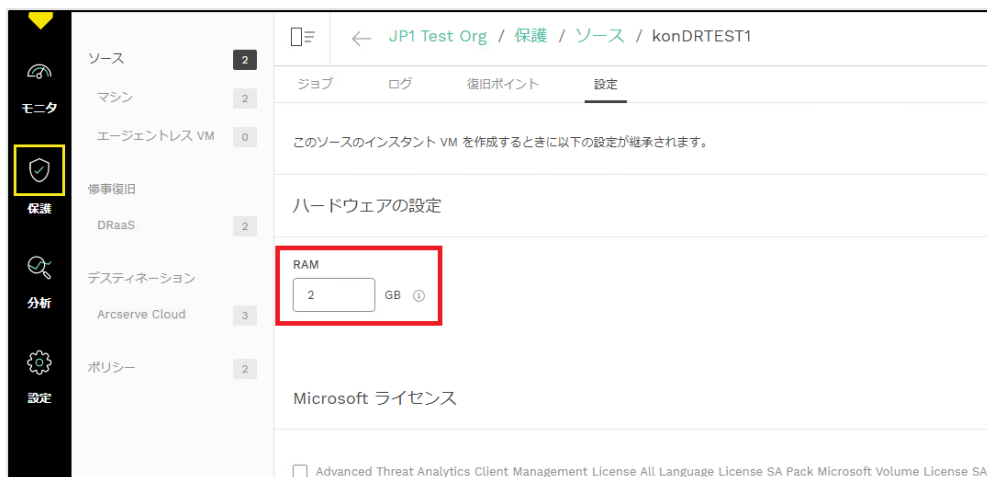
DRaaS 用ボリュームにバックアップを行うと、復旧ポイントを Arcserve クラウド内で本番システムの代替 VM としてすぐに起動できます。障害発生時に代替 VM を起動するには以下の要領でプロビジョニングを行います。

注意：プロビジョニング後はバックアップ運用が停止します。運用を再開したい場合は、代替 VM の電源をオフにした後でプロビジョニングを解除してください。

1. Cloud Console にログインし、[保護]-[DRaaS]をクリックします。
2. プロビジョニング対象マシン名の [アクション] カラムでプルダウンし、[ターゲット VM 環境設定]から、起動する VM のメモリを調整できます。



ご契約いただいている DRaaS のコンピュータ リソースから、2GB~128GB（偶数）のメモリを割り当てることができます。



3. プロビジョニング対象マシン名の [アクション] カラムでプルダウンし、[プロビジョニング] をクリックします。



4. プロビジョニングが開始された旨のメッセージが表示されます。対象マシンの [状態] フィールドが「実行」となるまで数分お待ちください。



7.2 復旧された VM へのリモート デスクトップ接続

プロビジョニングが完了した VM には、リモートデスクトップで接続が可能です。以下の手順で接続します。

1. Cloud Console にログインし、[保護] - [DRaaS] をクリックします。
2. 接続する VM の [アクション] カラムでプルダウンし、[リモート コンソール] をクリックします。



3. Web ブラウザで設定されているダウンロード保存先に、「RemoteConsole.rdp」ファイルがダウンロード/保存されます。



4. また、画面上部に、接続に使用するための認証情報が表示されます。

[パスワード]フィールドの文字列を選択し、コピーします。

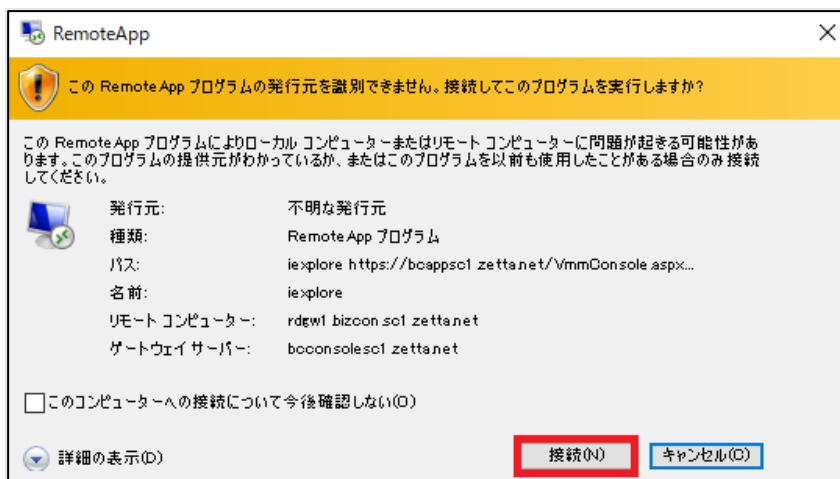


5. ダウンロードされた「RemoteConsole.rdp」を実行します。

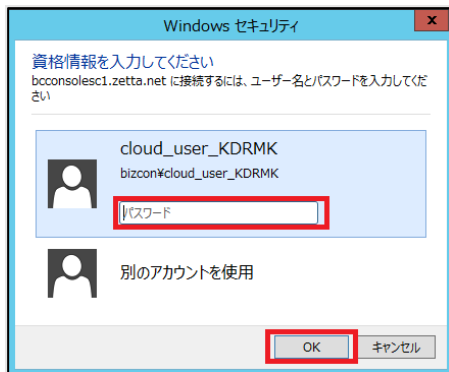
ご利用の環境によっては、セキュリティの警告メッセージが表示されます。

※接続先のパスやリモートコンピュータ、ゲートウェイとして“zetta”を含む文字列が表示されていますが、これは Cloud Direct の開発部門の旧称です。

[接続]をクリックします。

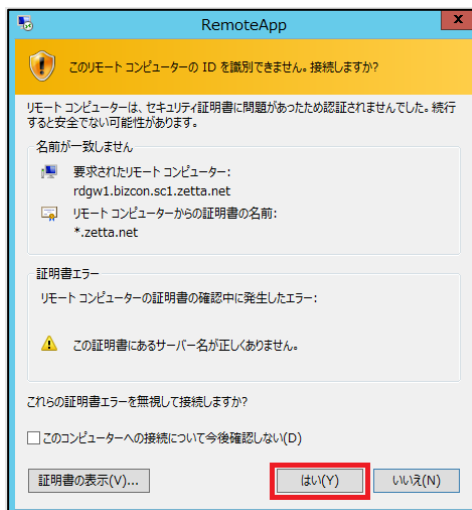


6. 資格情報の入力を促す画面が表示されます。フィールドに手順 2. でコピーしたパスワードを貼りつけて、[OK]をクリックします。

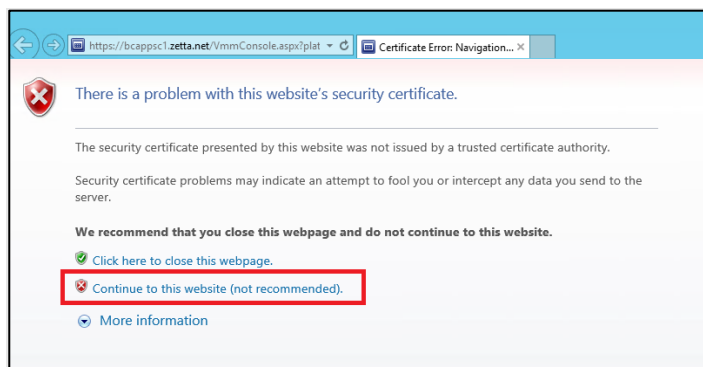


7. セキュリティ証明書に関するメッセージが表示されます。

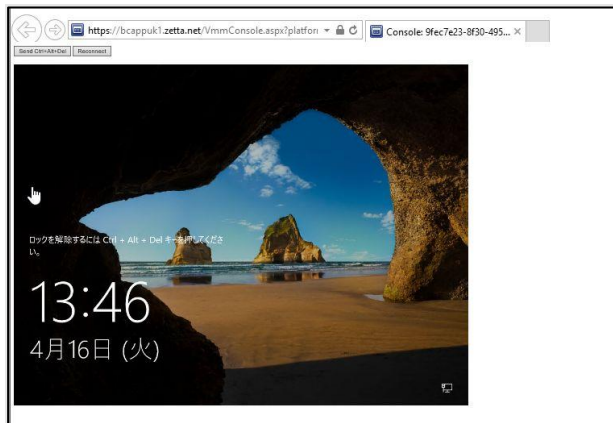
正しくサーバ証明書を用意いただいたうえでリモートデスクトップに接続します。この資料では評価目的のためそのまま[はい]をクリックしエラーを無視して接続します。



8. 環境によってはブラウザに以下の証明書に関するメッセージが表示される場合があります。この資料では評価目的のためそのまま [Continue to this website (not recommended)] をクリックします。



9. 接続が完了し、ログオン画面が表示されます。ログオンして動作を確認してください。



7.3 ポイント対サイト (Point to Site) の VPN 接続

ポイント対サイトの VPN 接続により、単一のノードから Arcserve クラウド上の環境に対してセキュアな仮想プライベート ネットワーク接続が可能となります。お客様環境のコンピュータから Arcserve クラウド上に復旧された VM と通信をする場合に利用できます。

ポイント対サイトの VPN 接続には「OpenVPN」ツールを利用します。

1. Cloud Console にログインし、[設定]-[ネットワーク設定]を開きます。
[説明の表示] をクリックします。



2. Open VPN の利用方法の解説ページが表示されます。説明に従い、ツールのインストールおよび設定を行ってください。

Point-to-Site VPN

Point-to-Site VPN では、VPN クライアントとクラウドの間でセキュアなネットワーク接続を確立して、クラウドでアクティブ化されているビジネス上の重要なサーバにアクセスできます。

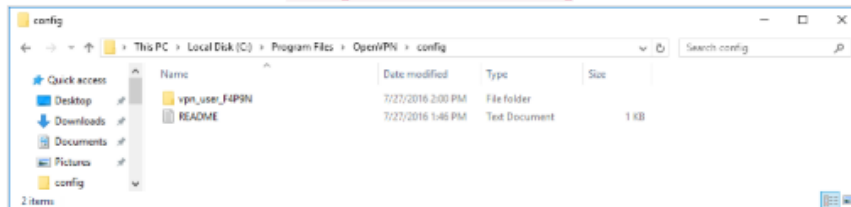
Windows Mac Linux

OpenVPN クライアントのダウンロードとインストール

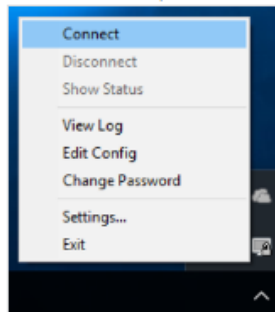
Windows OpenVPN クライアントのダウンロード に連絡してインストールすることもできます。

設定ファイルのダウンロードと展開

1. Windows 用の設定のダウンロード
2. 解凍した設定フォルダを以下に移動: `C:\Program Files\OpenVPN\config`

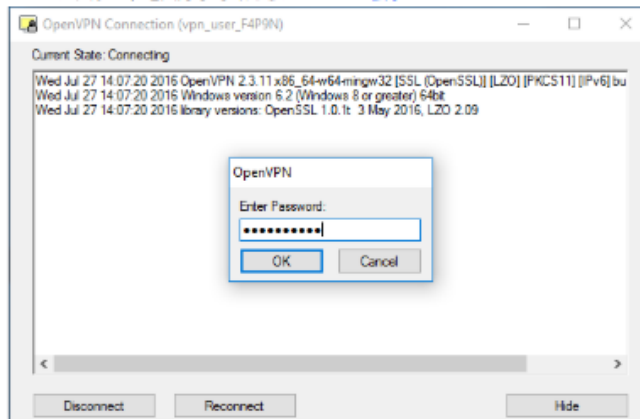


3. OpenVPN GUI を右クリックします。[接続] をクリックします (OpenVPN クライアントが現在実行中であることを前提としています)。



※画面上の「表示」をクリックするとパスワードを参照できます。

4. VPN パスワードを入力してください: ***** 表示



8 通常運用環境への切り戻し

8.1 フェイルバックの実行

フェイルバックは DRaaS において、クラウドから本番環境への切り戻しに使用する機能です。

ユーザが代替 VM 上で業務を行うことで、この VM には最新の業務データが蓄積されます。代替 VM からオンプレミスに運用を切り戻すには、代替 VM 上の最新業務データを含むイメージを本番環境にダウンロードする必要があります。

※ダウンロードしたイメージは既存環境にマウントしてデータを参照できます。

この、最新イメージのダウンロードの操作を「フェイルバック」と言います。

フェイルバックは、以下の3つのステップで実行されます。

STEP1.オンライン フル ダウンロード

クラウド上の代替 VM のスナップショットを取得し、フル イメージをダウンロードします。この処理は、VM の大きさに応じて時間がかかります。

STEP2. オンライン 増分ダウンロード

STEP1 のスナップショット取得以降の増分をダウンロードします。

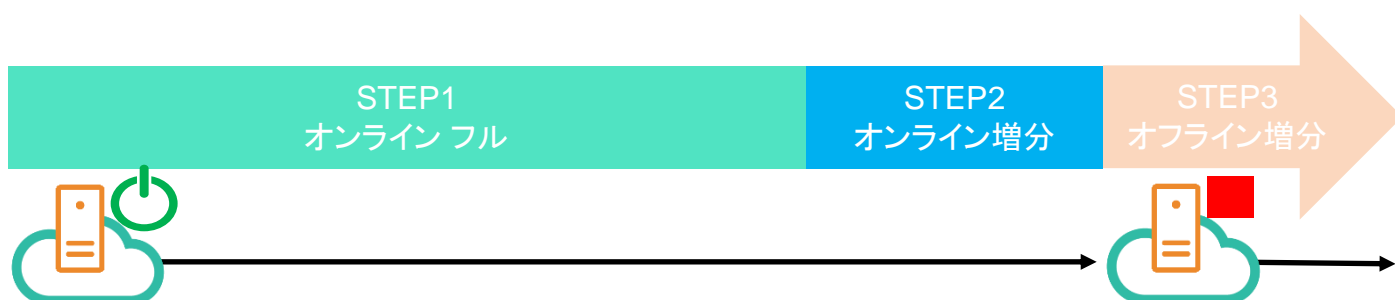
この処理は、STEP1 の後に自動的に実行されます。

STEP1 の実行中に行われた変更量に応じて時間がかかります。

STEP3. オフライン 増分ダウンロード

クラウド上の代替 VM をシャットダウンしてユーザアクセスを遮断し、STEP2.以降の増分をダウンロードします。

シャットダウン以降は代替 VM に変更が加えられないため、この処理は STEP2 実行からシャットダウンをするまでの変更分のみのダウンロードとなります。



以下は、フェイルバックの実行手順です。

STEP1.オンライン フル ダウンロード、および STEP2. オンライン 増分ダウンロード の実行

1. [保護]-[DRaaS]をクリックし、フェイルバックを実行したいクラウド上のVMの[アクション]カラムでプルダウンし、[フェイルバックを開始]をクリックします。

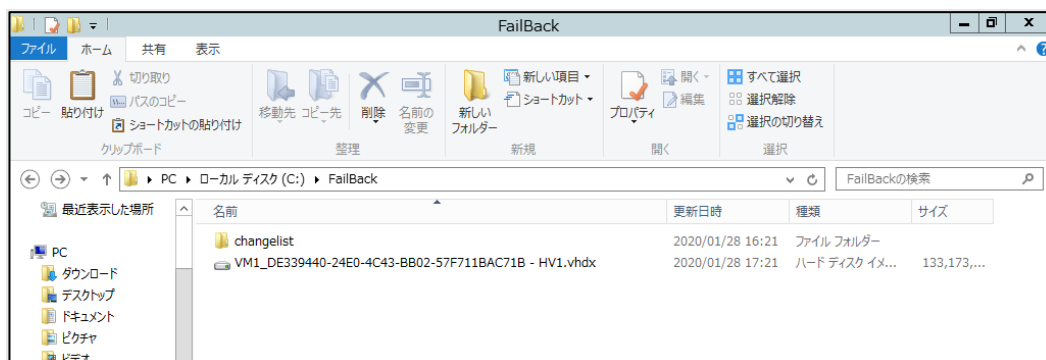


[デスティネーション システム]で、ダウンロード先となるシステム、[デスティネーション パス]として、デスティネーション システム上のリストア先となるディレクトリへのパス、[イメージ フォーマット]としてリストアされるイメージ ファイルの形式を指定し、[フェイルバックを開始]をクリックします。



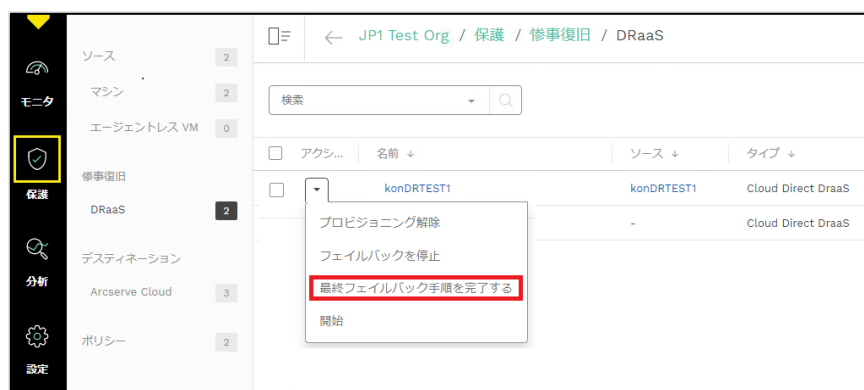
※リストアするイメージ ファイルの利用方法については、5.5.1 保護対象の設定内の、[<参考：アクティビティのタイプとリストア単位>](#)をご参照ください。

フェイルバック実行開始時点のフルイメージ、およびそれ以降の増分のダウンロードが行われます。※増分イメージはフルイメージに合成されます。



STEP3. オフライン 増分ダウンロード の実行

- ダウンロードが完了したことを確認し、クラウド上の VM をシャットダウンします。
- アクションカラムでプルダウンし [最終フェイルバック手順を完了する]をクリックします。



ダウンロードが完了したら、フェイルバックは完了です。ダウンロードしたイメージは既存環境にマウントしてデータを参照できます。

9 参考情報

- ・動作要件

<https://support.arcserve.com/s/article/115003836346?language=ja>

- ・Arcserve クラウド サービス規約

<https://www.arcserve.com/jp/cloud-services/>

- ・購入方法と価格

<https://www.arcserve.com/jp/licensing-options/>

- ・スタートアップ ガイド

【仮想エージェントレス 編】

<https://www.arcserve.com/sites/default/files/wp-doc/ucd-startup-guide-agentless.pdf>

【Linux 編】

<https://www.arcserve.com/sites/default/files/wp-doc/ucd-startup-guide-linux.pdf>

- ・オンライン ヘルプ

http://documentation.arcserve.com/Arcserve-Cloud/Available/JPN/Bookshelf_Files/HTML/olh/default.htm

- ・よくあるご質問と回答

<https://www.arcserve.com/sites/default/files/2022-05/ucd-faq.pdf>

- ・注意/制限事項

<https://support.arcserve.com/s/article/2019081401?language=ja>

- ・Arcserve Japan Direct (購入前のお問い合わせ)

フリーダイヤル： 0120-410-116 (平日 9:00~17:30 ※土曜・日曜・祝日・弊社定休日を除きます)

<https://www.arcserve.com/jp/contact-us/>

- ・Arcserve サポート ポータル

<https://support.arcserve.com/s/?language=ja>